AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

Manual de Utilização do Middleware do Cartão de Cidadão

FEVEREIRO DE 2012

Agência para a Modernização Administrativa, I.P.
www.ama.pt | ama@ama.pt
TEL.: (+351) 21 723 12 00
FAX: (+351) 21 723 12 55
R. Abranches Ferrão n. 10, 3º 1600-001 Lisboa - PORTUGAL

ÍNDICE

1 Introdução....4

2 Download, instalação e remoção do middleware....5

2.1 Sistemas Operativos oficialmente suportados....5

2.2 Instalação do middleware....5

2.2.1 Instalação em Microsoft Windows....5

2.2.2 Instalação em Linux....6

2.2.3 Instalação em MAC OS X....8

2.3 Remoção do Middleware 10

2.3.1 Remoção em Microsoft Windows....10

2.3.2 Remoção em Linux....11

2.3.3 Remoção em MAC OS X....11

3 Aplicação Utilitária....12

3.1 Apresentação da Aplicação....13

3.2 Funcionalidades da aplicação....14

3.2.1 Impressão e exportação para PDF dos dados do cartão de cidadão....14

3.2.2 Assinatura digital de ficheiros....16

3.2.3 Verificação da Assinatura digital de ficheiros....19

4 Integração com Autenticação em Sistemas Operativos....21

4.1 Autenticação em Microsoft Windows....21

4.2 Autenticação em Linux....29

4.2.1 Configurar o pam de forma a utilizar o módulo pkcs11....31

5 Notas do Utilizador....33

Autores e contribuidores		
Nome	Contacto	Data
André Guerreiro	andre.guerreiro@caixamagica.pt	
Rui Martinho	rui.martinho@ama.pt	
Vasco Silva	vasco.silva@caixamagica.pt	

Histórico de Revisões:			
Versão	Autor	Descrição	Data
0.1	Vasco Silva	Primeira versão do documento	13-02-12
1	Vasco Silva	Substituição do Template do documento	26-06-13

1 Introdução

O presente documento tem o objectivo de apresentar aos cidadãos as funcionalidades providenciadas pelo middleware do cartão de cidadão, e a respectiva utilização.

2 Download, instalação e remoção do middleware

Neste ponto são apresentadas as instruções para a instalação e remoção do middleware do cartão de cidadão.

O middleware do cartão de cidadão é oficialmente suportado para os sistemas operativos Windows, Linux e MAC OS X. No ponto seguinte são detalhados os sistemas operativos e versões oficialmente suportadas:

2.1 Sistemas Operativos oficialmente suportados

A lista de sistemas operativos suportados, nas suas arquitecturas de 32 e 64 bits, são apresentados abaixo:

- Microsoft Windows
- Windows Vista / 7
- Windows XP
- Linux
- Caixa Mágica 15 / 16 /17
- CentOS 6
- Fedora 15 / 16
- OpenSuse 11.4 / 12.1
- Ubuntu 10.04 / 11.04
- MAC OS X
- Lion
- Snow Leopard
- Leopard

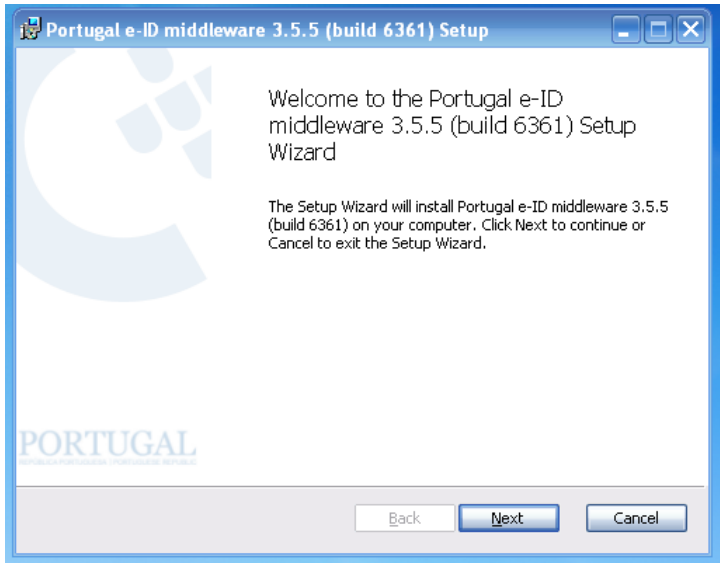
2.2 Instalação do middleware

Para a instalação do middleware do Cartão de cidadão, deverá executar passos descritos nos pontos seguintes, respectivos ao sistema operativo que está a utilizar.

2.2.1 Instalação em Microsoft Windows

1. Download do pacote de instalação: Descarregar o seguinte ficheiro da Internet: http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/lastversion/PteidMW-Basic.msi

2. Executar o pacote de instalação: Após ter descarregado o ficheiro acima referido, deverá fazer duplo clique sobre este, e surgirá um ecrã semelhante ao apresentados de seguida:



3. Ao ver este ecrã, deverá clicar no botão Next até concluir a instalação.

4. Após a conclusão deste assistente, este solicitará a reinicialização do computador.

5. No próximo arranque do windows a instalação do middleware estará finalizada.

2.2.2 Instalação em Linux

1. Download do pacote de instalação. Para efectuar o download do pacote de instalação específico para a respectiva versão de Linux, deverá seguir a tabela de download no URL http://svn.gov.pt/projects/ccidadao/wiki
   Neste link encontrará uma tabela idêntica à apresentada na imagem da página seguinte, onde estão apresentados os links de download para a última versão do middleware.

Instalação da versão Offline

A instalação da versão Offline do middleware, está disponível para vários sistemas operativos em formato de pacotes de instalação. Poderá assim descarregar os pacotes preparados para instalação na seguinte localização:

http://svn.gov.pt/projects/ccidadao/browser/middleware-offline/tags/builds

Sistema Operativo	Arquitectura	URL para download
Linux		
Caixa Mágica 14, 15	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/rpm/Mandriva_2009.1/pteid-mw_0.9-2_i586.rpm
Caixa Mágica 14, 15	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/rpm/Mandriva_2009.1/pteid-mw_0.9-2_x86_64.rpm
Caixa Mágica 16, 17	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/deb/pteid-mw_0.9-2_i386.deb
Caixa Mágica 16, 17	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/deb/pteid-mw_0.9-2_amd64.deb
Fedora 15	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/rpm/Fedora_15/pteid-mw_0.9-2_i386.rpm
Fedora 15	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/rpm/Fedora_15/pteid-mw_0.9-2_x86_64.rpm
Fedora 16	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/rpm/Fedora_16/pteid-mw_0.9-2_i386.rpm
Fedora 16	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/rpm/Fedora_16/pteid-mw_0.9-2_x86_64.rpm
Ubuntu 10.04, 11.10	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/deb/pteid-mw_0.9-2_i386.deb
Ubuntu 10.04, 11.10	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/deb/pteid-mw_0.9-2_i386.deb
Microsoft Windows		
Windows Vista / 7	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/win32/pteid-mw_0.9-2.msi
Windows Vista / 7	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/win32/pteid-mw_0.9-2.msi
Windows XP	x86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/win32/pteid-mw_0.9-2.msi
Windows XP	x86_64	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/win32/pteid-mw_0.9-2.msi
MAC OSx		
Lion	x86_64 / X86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/macos/pteidgui.dmg
Snow Leopard	x86_64 / X86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/macos/pteidgui.dmg
Leopard	x86_64 / X86	http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/macos/pteidgui.dmg

2. Após fazer o download dos ficheiros, estes poderão ser de extensão .rpm ou .deb, consoante a distribuição seleccionada.

3. Inicie uma linha de comandos, e navegue até à directoria onde se encontram os ficheiros para instalação.
   ex.:

```
cd /home/user/Download
```

4. Execute o comando de instalação de software no sistema, consoante a extensão dos ficheiros transferidos:
   Ficheiros de extensão .deb, execute o comando:

```
sudo dpkg -i *.deb
```

   Ficheiros de extensão .rpm, execute o comando:

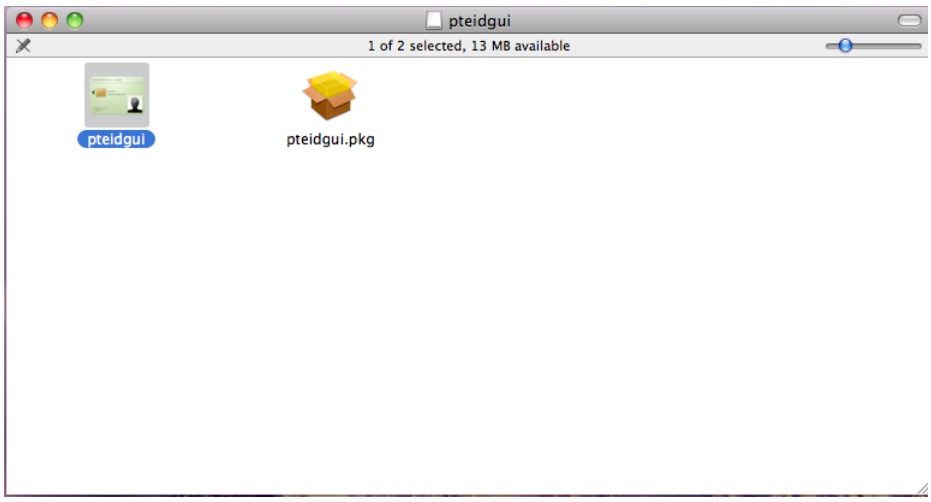
```
sudo rpm -ivh *.rpm
```

5. Após a execução dos passos acima o Middleware do cartão de cidadão ficará instalado no computador e pronto a ser utilizado.

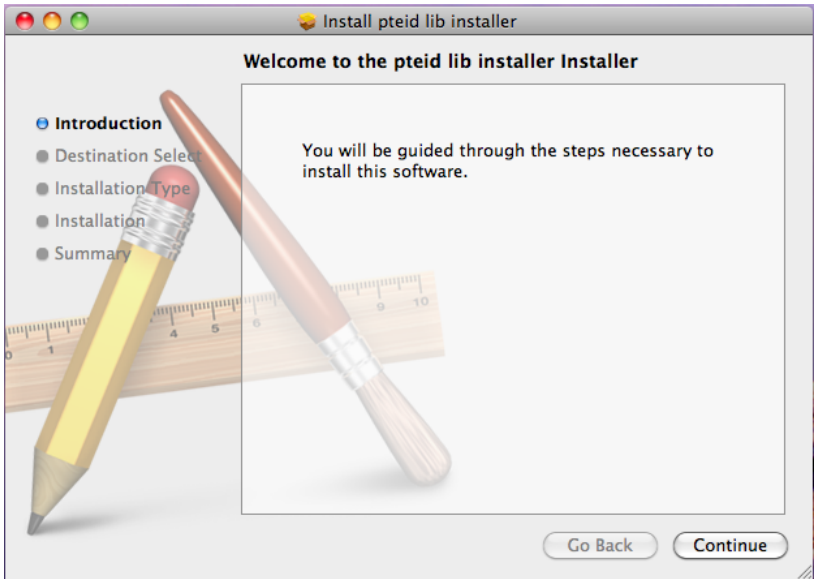
2.2.3 Instalação em MAC OS X

1. Download do pacote de instalação: Descarregar o seguinte ficheiro da Internet: http://svn.gov.pt/projects/ccidadao/repository/middleware-offline/tags/builds/macos/pteidgui.dmg

2. Executar o pacote de instalação: Após ter descarregado o ficheiro acima referido, deverá fazer duplo clique sobre este, e surgirá um ecrã semelhante ao apresentado de seguida:



3. Faça duplo clique sobre o ficheiro pteidgui.pkg. Será-lhe apresentado o seguinte ecrã:



4. Ao ver este ecrã, deverá clicar no botão Continue até concluir a instalação.

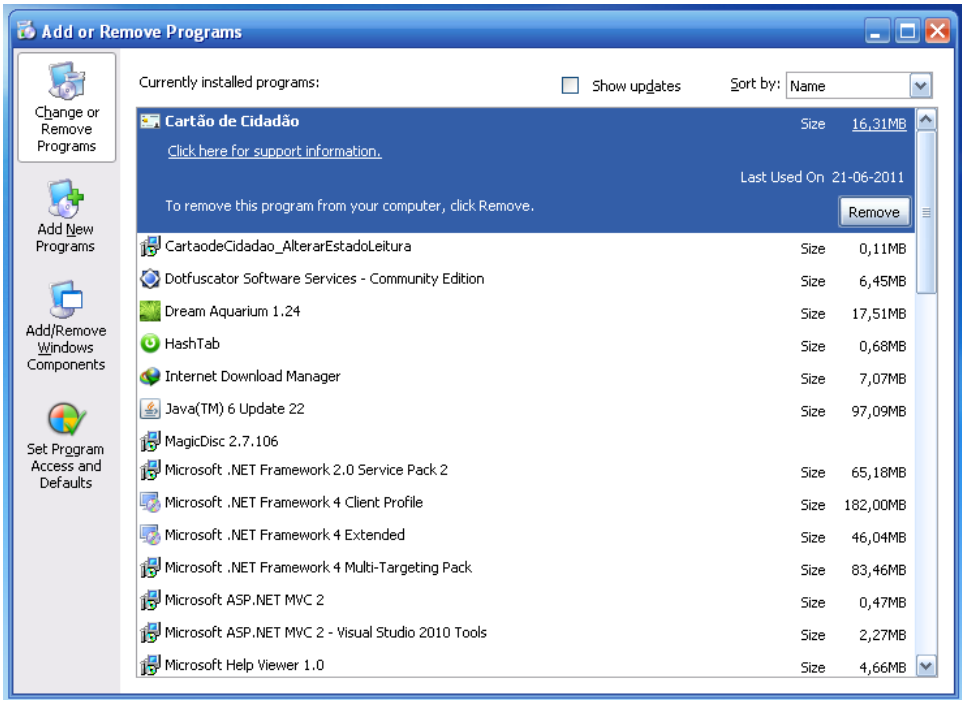
5. Após a conclusão deste assistente, o Middleware ficará instalado no computador. É apenas necessário copiar o atalho para a aplicação, para o local que o utilizador pretenda. Para isso basta arrastar o ícone pteidgui para o destino pretendido.

2.3 Remoção do Middleware

Para proceder à remoção do middleware do cartão de cidadão, deverá executar passos descritos nos pontos seguintes, respectivos ao sistema operativo que está a utilizar.

2.3.1 Remoção em Microsoft Windows

1. Aceda ao Painel de Controle;
2. Selecione a Opção Adicionar ou Remover Programas.
3. No ecrã apresentado, selecione o programa Cartão de Cidadão, conforme apresentado na janela seguinte:



4. Clique em Remover. Confirme todas as janelas de diálogo que irão surgir.
5. Após estes passos, o middleware foi removido do computador. É recomendável que esta seja reiniciado no final destes passo.

2.3.2 Remoção em Linux

1. Execute o comando de remoção de software no sistema, consoante o gestor de pacotes utilizado pelo seu sistema.
   Gestor de pacotes baseado em ficheiros .deb, execute o comando:

```
sudo dpkg -r pteid-mw xul-ext-pteidpkcs11 xul-ext-pteidcertinstall
```

   Gestor de pacotes baseado em ficheiros .rpm, execute o comando:

```
sudo rpm -U pteid-mw xul-ext-pteidpkcs11 xul-ext-pteidcertinstall
```

2. Após este passo, o middleware foi removido do computador.

2.3.3 Remoção em MAC OS X

1. Navegue até à directoria onde foi colocado o atalho pteidgui.
2. Selecione o ficheiro pteidgui e arraste-o para o caixote do lixo.
3. Após estes passos, o middleware foi removido do computador.

3 Aplicação Utilitária

A aplicação Utilitária pode ser utilizada para visualizar e gerir os dados no cartão.

Com esta aplicação poderá executar as seguintes operações:

- Visualização da informação e foto do cidadão;
- Visualização da morada do cidadão;
- Visualização dos certificados do Estado e do cidadão;
- Registo dos certificados do Estado e do cidadão;
- Gestão de PINs (Testar PIN, Alterar PIN);
- Gestão Pasta Pública;
- Criação e validação de assinaturas digitais de ficheiros.
- Entre outros.

O aspecto e comportamentos da aplicação é semelhante para os três tipos de sistemas operativos, à excepção de algumas funcionalidades de registo de certificados. Esta está apenas disponível em Windows, visto esta funcionalidade nativa, ser específica do sistema operativo Microsoft Windows.

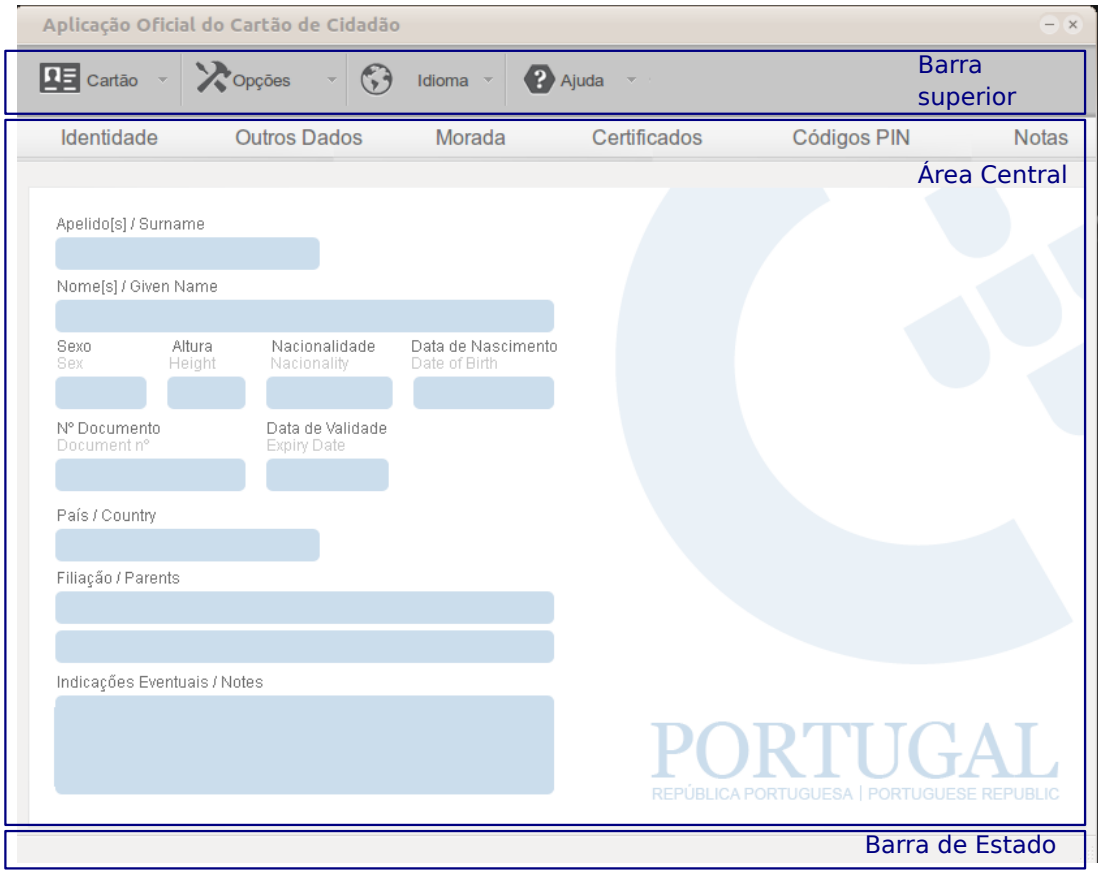
O atalho para a aplicação fica disponível em localizações diferentes consoante o tipo de sistema operativo:

- Em Windows surgirá em: Iniciar → Programas → Cartão de Cidadão
- Em Linux surgirá em Aplicações → Acessórios → Cartão de Cidadão
- Em MAC OS X, surgirá na localização escolhida pelo utilizador durante o processo de instalação.

3.1 Apresentação da Aplicação

A aplicação é composta por 3 áreas principais de interacção:

- Barra superior: São disponibilizadas várias acções agrupadas por menús;
- Área Central: Permite ao utilizador visualizar os dados do cartão de cidadão. Esta visualização está agrupada por conjuntos de dados, cada conjunto possui o respectivo separador;
- Barra de estado: Apresenta ao utilizador mensagens sobre o estado da aplicação, conforme as acções executadas.



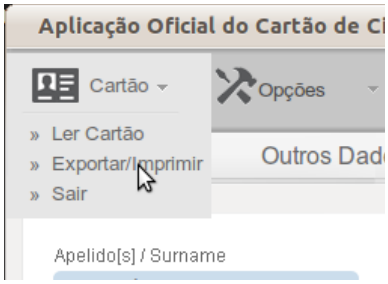
3.2 Funcionalidades da aplicação

3.2.1 Impressão e exportação para PDF dos dados do cartão de cidadão

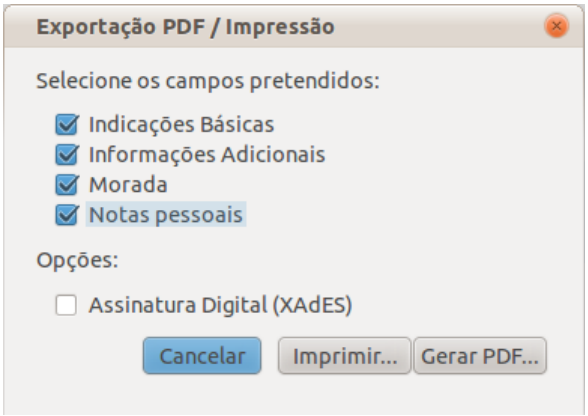
A aplicação permite a exportação dos dados do cartão de cidadão para um documento no formato PDF ou a impressão directa do documento.

Para executar estas operações deverá executar os seguintes passos:

1. Na Barra superior, seleccionar dentro do menu “Cartão” a opção “Exportar / Imprimir”:



2. Após clicar na opção acima referida, surgirá o seguinte ecrã:



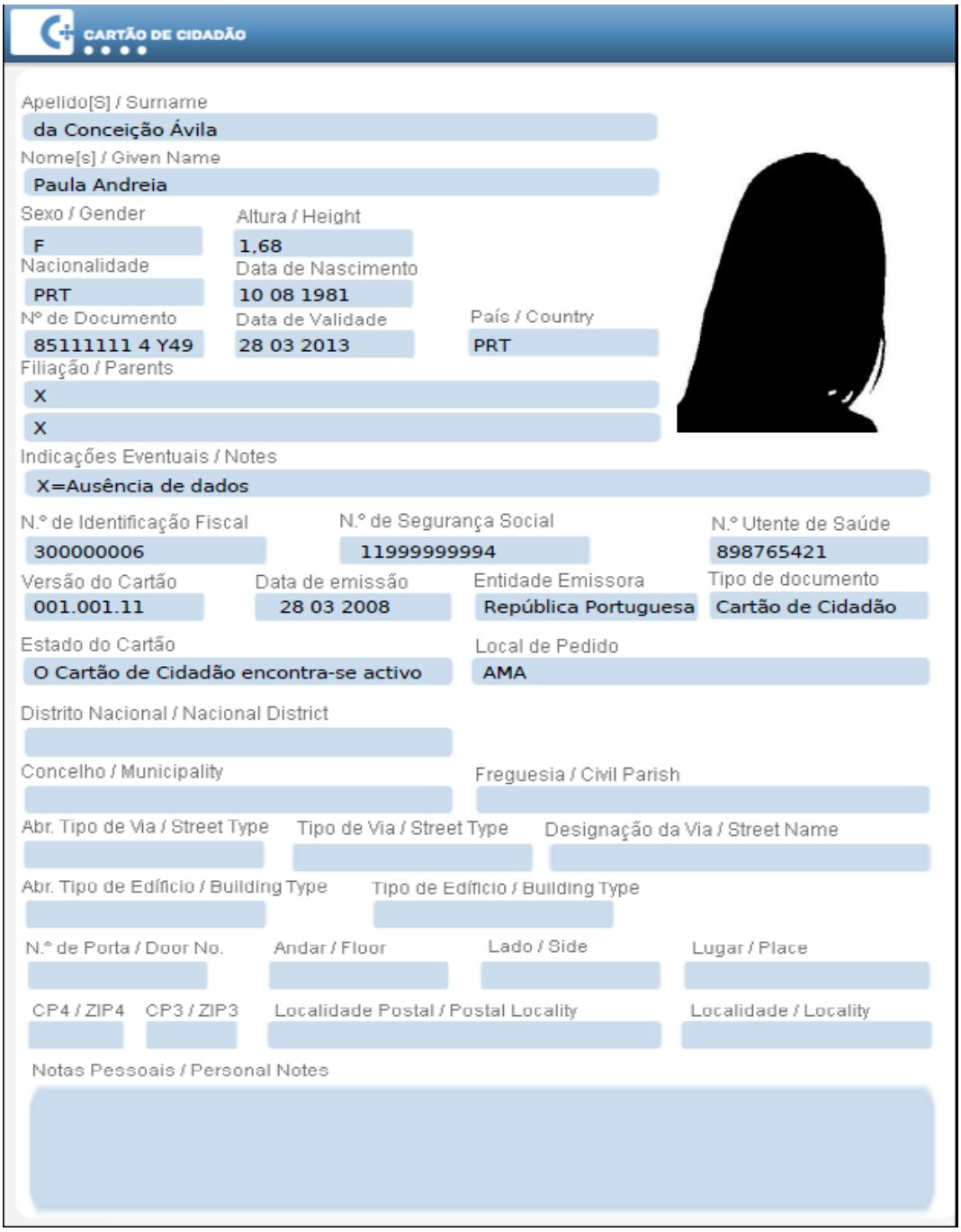
   Neste ecrã deverá seleccionar os grupos de campos a incluir no documento. No exemplo acima foram seleccionados todos os grupos de campos.

   Assinatura Digital (XadES): Esta opção é aplicável apenas para o caso de exportação para PDF e permite assinar digitalmente o documento exportado no formato Xades.

3. Após seleccionar os campos pretendidos, poderá então “Imprimir” ou “Gerar PDF”. Para concluir a operação, clique no botão respectivo à operação que pretende efectuar.

4. O documento a ser exportado e/ou impresso terá um aspecto gráfico conforme o apresentado na página seguinte.

Aspecto gráfico do documento a exportar / imprimir:



CARTÃO DE CIDADÃO

Apelido[S] / Surname: da Conceição Ávila
Nome[s] / Given Name: Paula Andreia
Sexo / Gender: F
Altura / Height: 1,68
Nacionalidade: PRT
Data de Nascimento: 10 08 1981
Nº de Documento: 85111111 4 Y49
Data de Validade: 28 03 2013
País / Country: PRT
Filiação / Parents: X
X
Indicações Eventuais / Notes: X=Ausência de dados
N.º de Identificação Fiscal: 300000006
N.º de Segurança Social: 11999999994
N.º Utente de Saúde: 898765421
Versão do Cartão: 001.001.11
Data de emissão: 28 03 2008
Entidade Emissora: República Portuguesa
Tipo de documento: Cartão de Cidadão
Estado do Cartão: O Cartão de Cidadão encontra-se activo
Local de Pedido: AMA
Distrito Nacional / Nacional District
Concelho / Municipality
Freguesia / Civil Parish
Abr. Tipo de Via / Street Type
Tipo de Via / Street Type
Designação da Via / Street Name
Abr. Tipo de Edifício / Building Type
Tipo de Edifício / Building Type
N.º de Porta / Door No.
Andar / Floor
Lado / Side
Lugar / Place
CP4 / ZIP4
CP3 / ZIP3
Localidade Postal / Postal Locality
Localidade / Locality
Notas Pessoais / Personal Notes

3.2.2 Assinatura digital de ficheiros

A funcionalidade de assinatura foi desenhada de forma a facilitar a sua utilização no dia a dia. São de realçar algumas características como:

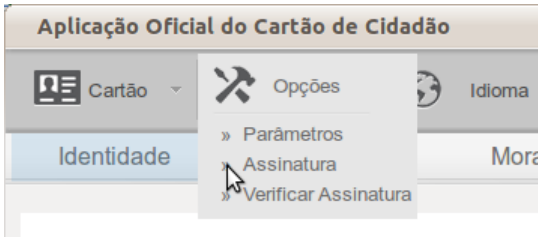
- **Assinatura de qualquer tipo de ficheiro:** A assinatura digital é guardada num ficheiro que irá acompanhar o ficheiro original, de forma a permitir a assinatura de qualquer tipo de ficheiro, sem alterar o seu conteúdo original.
- **Assinatura múltipla:** A funcionalidade de assinatura múltipla de documentos permite ao utilizador assinar inúmeros documentos simultâneamente, sem que tenha que inserir o respectivo PIN diversas vezes.
- **Assinatura individual ou conjunta:** Ao efectuar uma assinatura múltipla de documentos o utilizador pode escolher se pretende a assinatura conjunta (uma única assinatura, onde são incluídos todos os ficheiros), ou a assinatura individual de ficheiros (uma assinatura para cada ficheiro).

  Estas opções deverão ser utilizadas, consoante a utilização final que se pretenda aplicar aos ficheiros em causa:

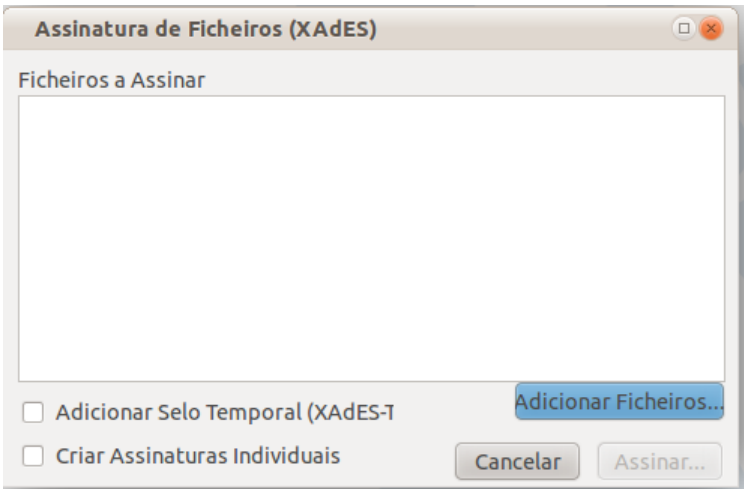
  - Vários ficheiros para o mesmo destinatário: deverá ser utilizada a assinatura conjunta, pois desta forma o destinatário poderá validar todos os documentos num único passo.
  - Vários ficheiros para diferentes destinatários: deverá ser utilizada a assinatura individual, pois desta forma será possível distribuir os vários ficheiros por diversos destinatários, e estes poderão assim validar os documentos individualmente.
- **Selo temporal:** Conforme o nome indica, consiste num selo temporal que é introduzido na assinatura do ficheiro. Desta forma, é possível provar a existência de determinado ficheiro à data que está inserida na assinatura. Este selo temporal utiliza o relógio dos serviços de assinatura digital.

Para assinar ficheiros, deverá assim proceder aos seguintes passos:

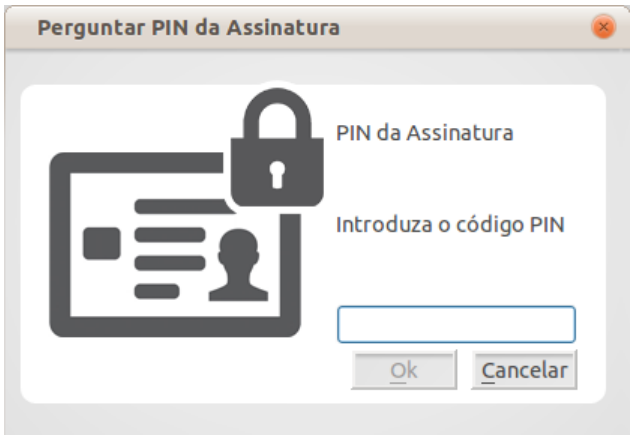
1. Na Barra superior, seleccionar dentro do menu “Opções” a opção “Assinatura”:



2. Após clicar na opção acima referida, surgirá o seguinte ecrã:

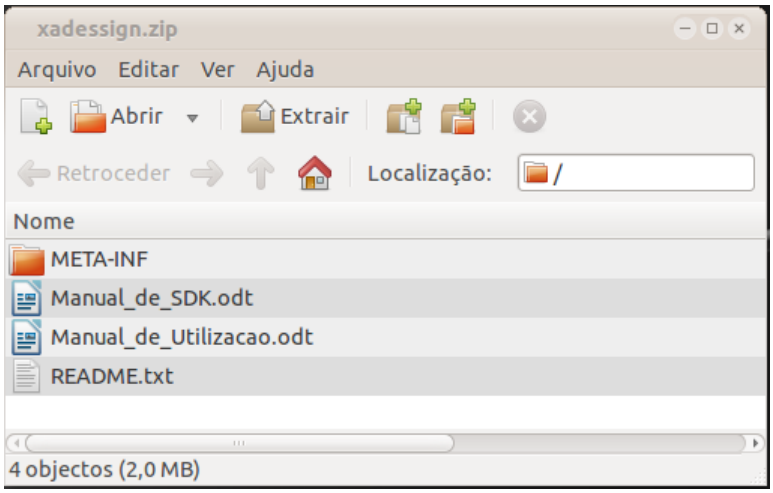


3. Ao clicar no botão “Adicionar Ficheiros”, irá surgir uma janela selecção de ficheiros, e nessa poderá seleccionar os ficheiros que pretende assinar.
   Para adicionar o selo temporal à assinatura, activar a respectiva caixa de selecção “Adicionar Selo Temporal (Xades-T)”.
   Caso pretenda assinar cada ficheiro individualmente, deverá activar a caixa de selecção “Criar Assinaturas Individuais”.
4. Após seleccionar os ficheiros a assinar, e as opções pretendidas, deverá clicar no botão “Assinar”;
5. Surgirá uma janela de navegação do sistema, onde deverá definir a localização e o nome do novo ficheiro .zip onde ficarão os ficheiros assinados e a respectiva assinatura. O nome por omissão deste ficheiro é “xadessign.zip”.
6. Após o passo anterior será pedido o PIN de autenticação para proceder à assinatura dos ficheiros:



7. Após o PIN de Assinatura ter sido correctamente introduzido, será então criado o ficheiro de assinatura. Os ficheiros foram assim assinados com sucesso!
   O ficheiro de assinatura consiste num ficheiro zip, e o seu conteúdo será o seguinte:
   - META-INF: Informação essencial da assinatura. Esta directoria não pode ser removida.
   - README.txt: Ficheiro de informações sobre a assinatura e instruções de validação.
   - Ficheiros Assinados: Todos os ficheiros assinados ficarão guardados dentro do ficheiro zip.

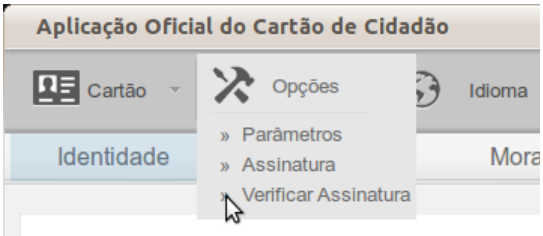
O conteúdo do ficheiro zip, de uma assinatura de dois ficheiros: “Manual_de_SDK.odt” e “Manual_de_Utilizacao.odt” será o seguinte:



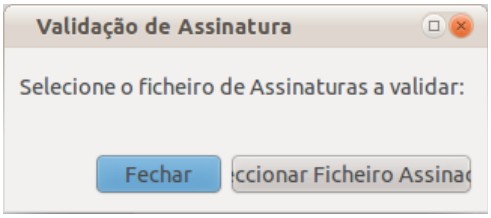
3.2.3 Verificação da Assinatura digital de ficheiros

Os passos necessário para a verificação de uma assinatura electrónica são os seguintes:

1. Na Barra superior, seleccionar dentro do menu “Opções” a opção “Verificar Assinatura”:



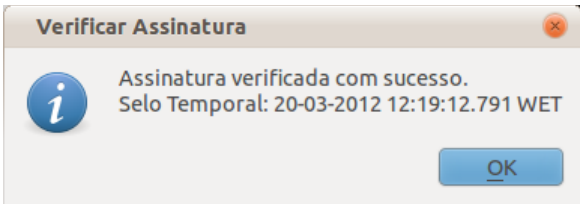
2. Após clicar na opção acima referida, surgirá o seguinte ecrã:



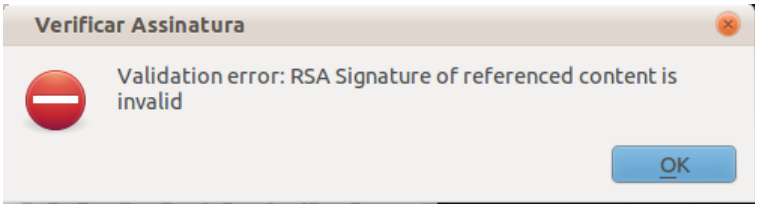
   Deverá clicar no botão “Selecionar Ficheiro Assinado”, e selecionar o ficheiro zip que pretende validar

3. Os resultados possíveis da validação da assinatura serão os seguintes:

   - Assinatura válida: A assinatura está válida, assegurando assim que o conteúdo dos ficheiros não foi modificado. Se a assinatura tiver sido gerada com selo temporal, este será apresentado neste caso:

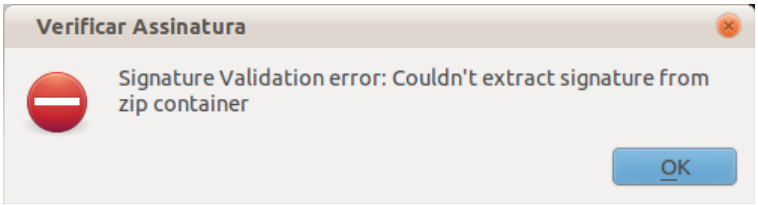


   - Assinatura inválida - Ficheiros modificados: Este erro na validação significa que os conteúdos dos ficheiros foram alterados após a



assinatura:

- Verificação impossível – Falta de ficheiros de assinatura: Este erro ocorre quando os ficheiros que deveriam estar dentro da directoria "META-INF" não são encontrados:



4 Integração com Autenticação em Sistemas Operativos

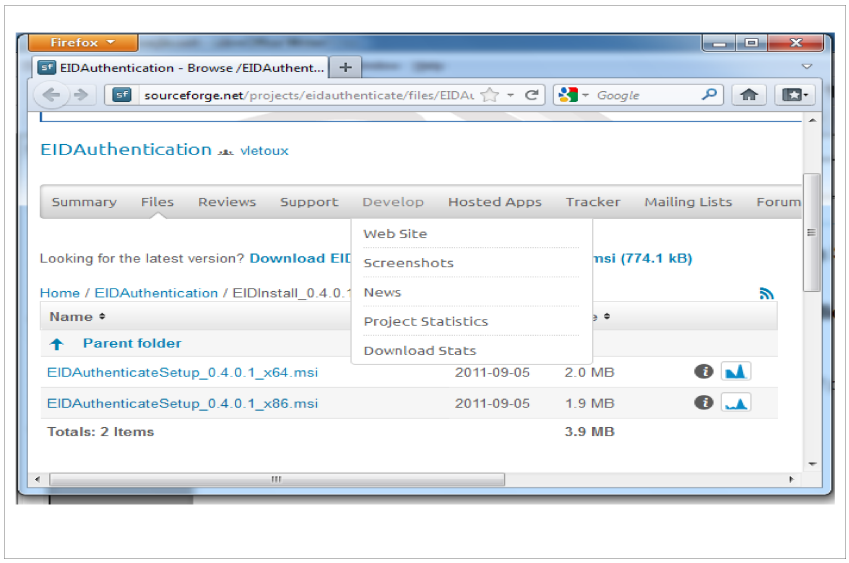
4.1 Autenticação em Microsoft Windows

A autenticação em Microsoft Windows 7 pode ser realizada utilizando um projecto externo chamado - EidAuthenticate (da autoria de Vincent LeThoux). Esta ferramenta contorna alguns parâmetros, sem causar danos no Windows que permite ao utilizador realizar o login com o Cartão de Cidadão utilizando este middleware.

Para instalar este software e realizar o login usando o Cartão de Cidadão deve seguir os seguintes passos:

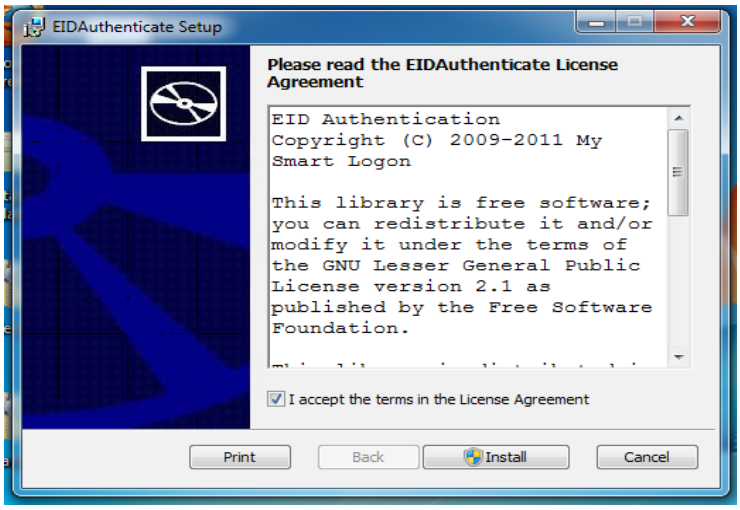
1- Abra o seu Navegador Web preferido e introduza o endereço *http://sourceforge.net/projects/eidauthenticate/files/EIDAuthentication/EIDInstall_0.4.0.1/* .

Nessa página(figura X) selecione o ficheiro para Download EIDAuthenticateSetup_0.4.0.1_x86.msi, caso tenha um sistema 32bits ou EIDAuthenticateSetup_0.4.0.1_x64.msi caso tenha um sistema 64bits.



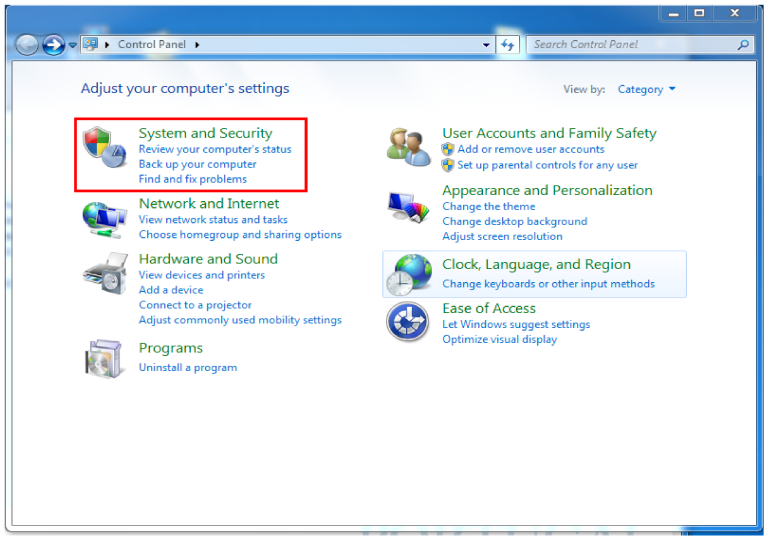
2 - Após proceder à descarga do ficheiro, na mesma pasta, execute o ficheiro para iniciar o assistente de instalação.

Siga as instruções do instalador e instale a aplicação EidAuthenticate.



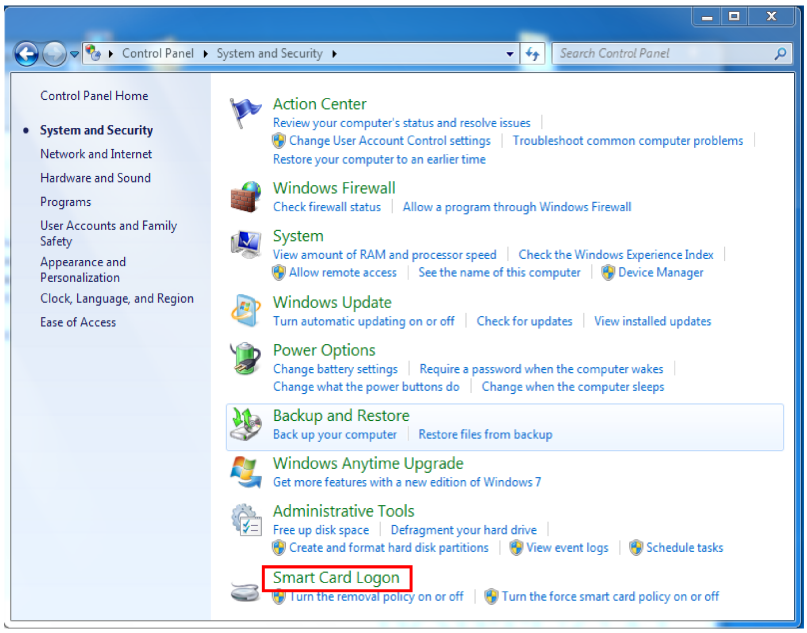
3 – Após a instalação é necessário efectuar a configuração do login de modo a utilizar o Cartão de Cidadão. O seguinte conjunto de imagens descreve o procedimento necessario. O cartão de cidadão deverá estar no leitor.

No painel de controlo seleccionar ***System and Security***



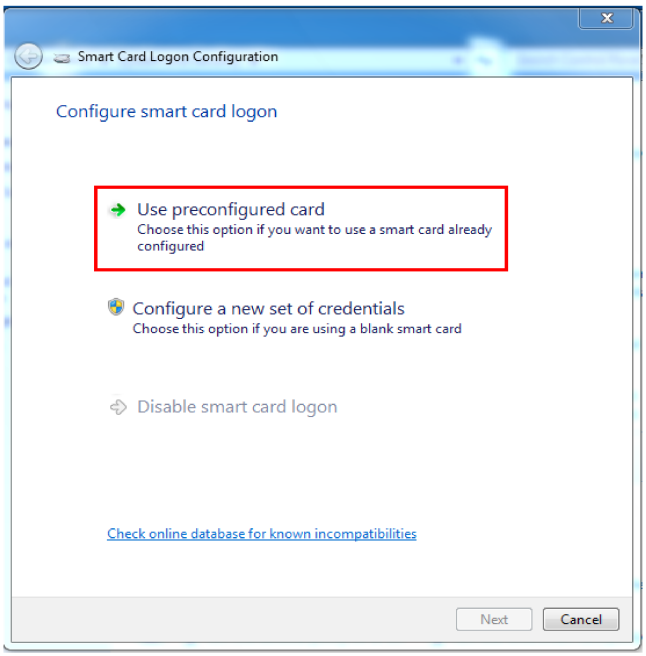
Painel de controlo

Seleccionar **Smart Card Logon**



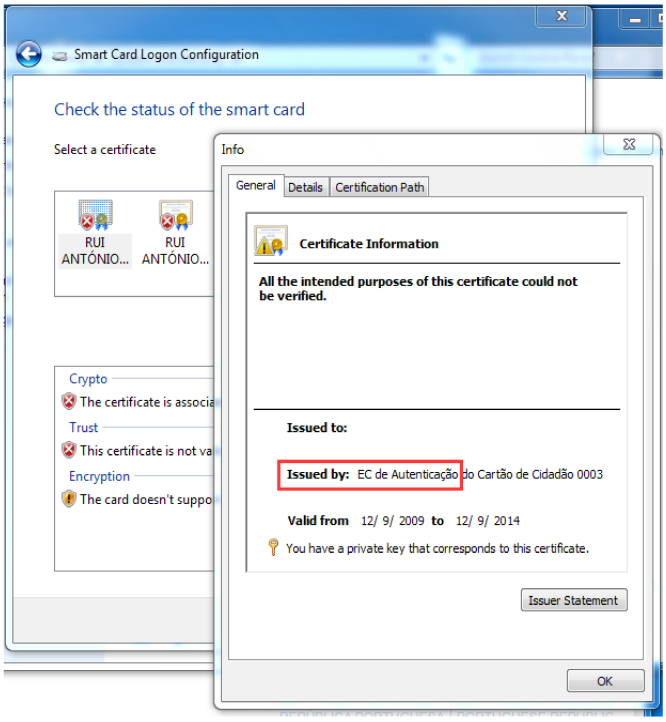
Painel de controlo - System Security

Seleccionar **Use preconfigured card**



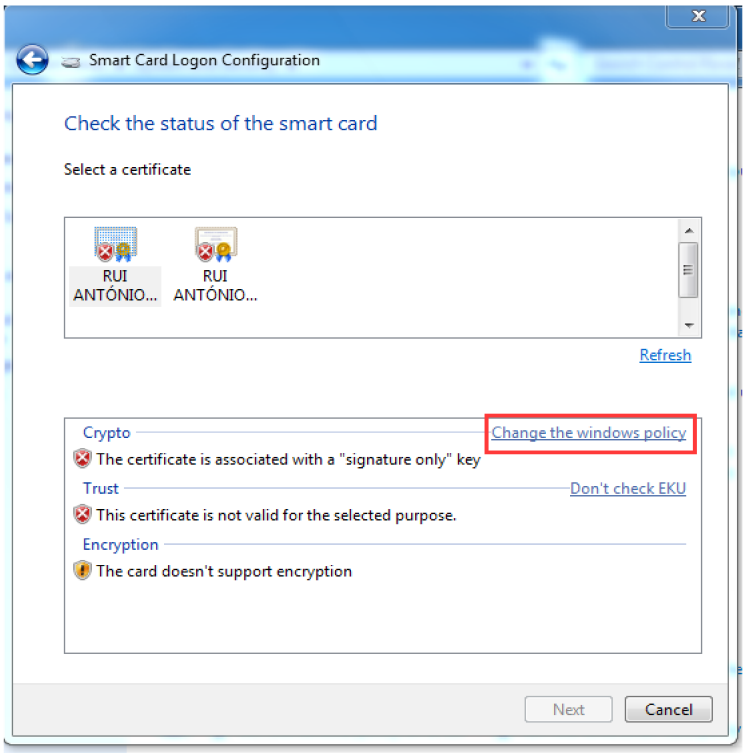
Configuração

Serão exibidos dois certificados relativos à autenticação e assinatura digital, deverá ser utilizado o certificado de autenticação (duplo clique em cima do certificado abre uma janela onde é possivel identificar o certificado)



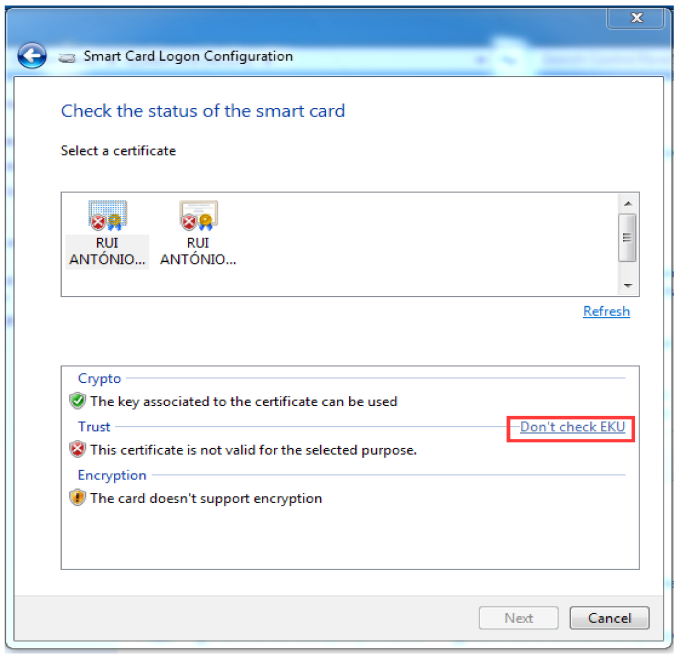
Janela de informação do certificado

Seleccionar a opção ***Change the windows policy***



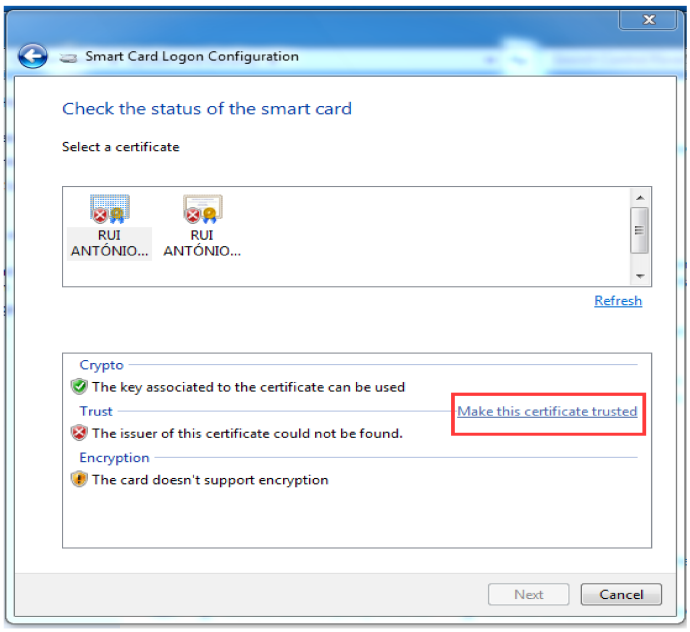
Change the windows policy

Seleccionar opção ***Don't check EKU***



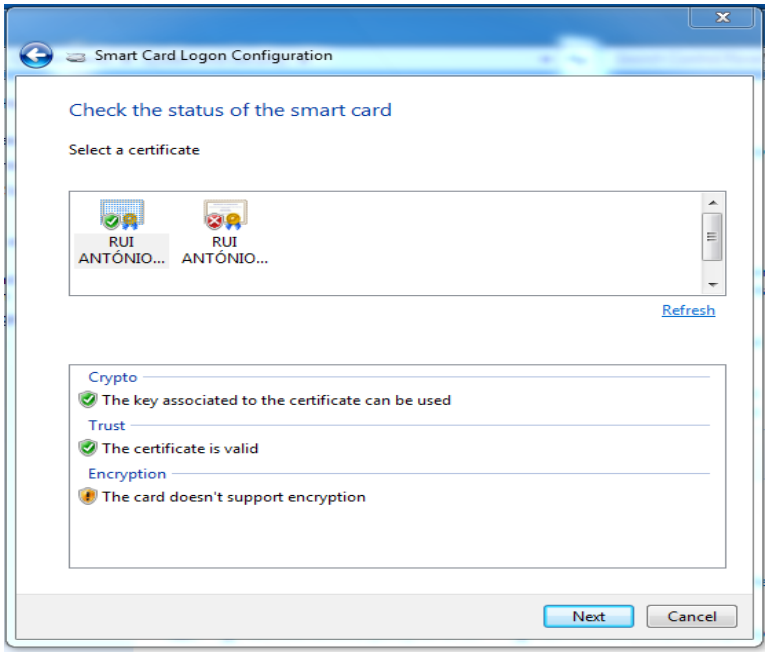
Don't check EKU

Seleccionar opção ***Make this certificate trusted***

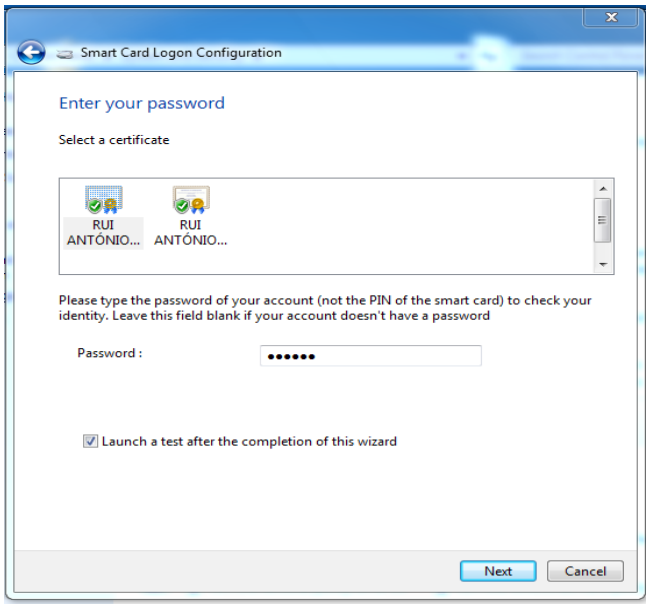


Make this certificate trusted

Após a realização deste procedimento o botão ***Next*** ficará activo e deverá ser seleccionado para proceder ao próximo passo.

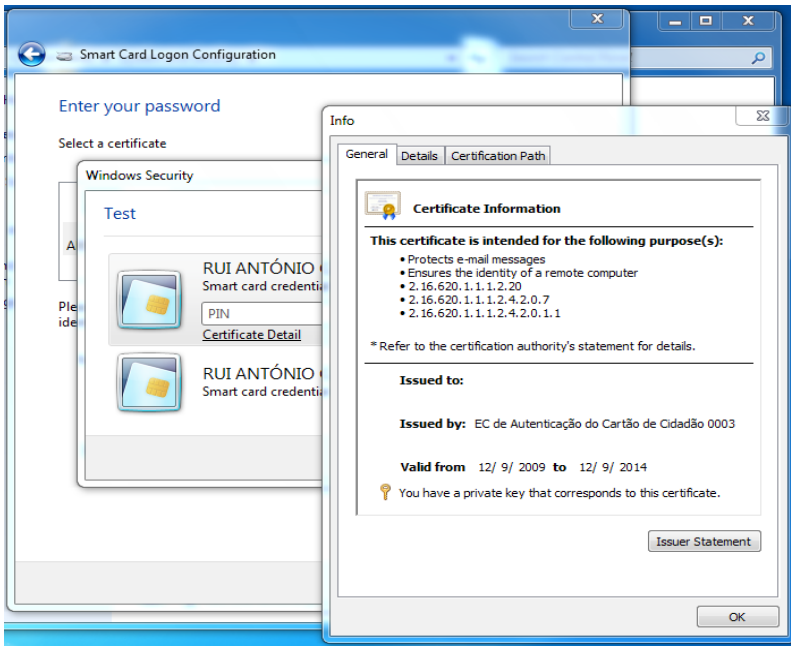


Seleccionar o certificado utilizado neste procedimento, introduzir a palavra passe do utilizador, manter a opção ***Launch a test after the completion of this wizard*** seleccionada, de modo efectuar um teste, premir botão ***Next***

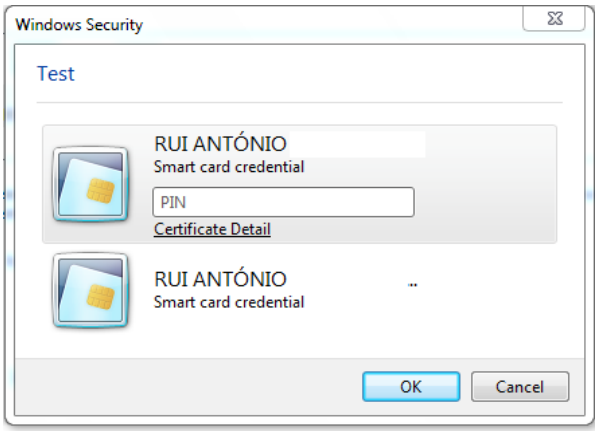


Será exibido um menu onde é possível seleccionar um dos dois certificados existentes no Cartão de Cidadão e introduzir o PIN correspondente.

Para este efeito de autenticação em Windows é indiferente qual o certificado utilizado bastando para tal estar configurado – ver passos anteriores). Para identificar o certificado basta premir a opção ***Certificate Detail***.



Introduzir o PIN



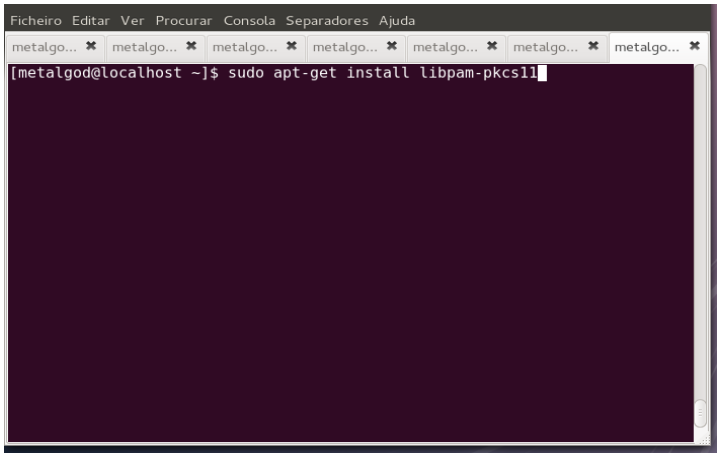
Após este passo a configuração da Autenticação em Windows Vista/7 está concluída.

4.2 Autenticação em Linux

A autenticação em Linux é feita através do *pam* (***Pluggable Authentication Module)***, que nos oferece a funcionalidade de autorização dinâmica e serviços nos sistemas *Linux.* Para utilizarmos o Cartão de Cidadão com o *pam* é necessário recorrer ao modulo *pkcs11* para interagir com o cartão.

Para tal é necessário instalar o suporte para *pkcs11* no *pam* e em sistemas Ubuntu/Debian/CaixaMágica devemos realizar o seguinte comando num terminal:

```
sudo apt-get install libpam-pkcs11
```



Após a instalação devemos criar as seguintes directorias.

```
sudo mkdir /etc/pam_pkcs11
sudo mkdir /etc/pam_pkcs11/cacerts
sudo mkdir /etc/pam_pkcs11/crls
```

De seguida deve copiar os certificados instalados pelo middleware no modulo pkcs11 de modo a completar a cadeia de certificação com os seguintes comandos:

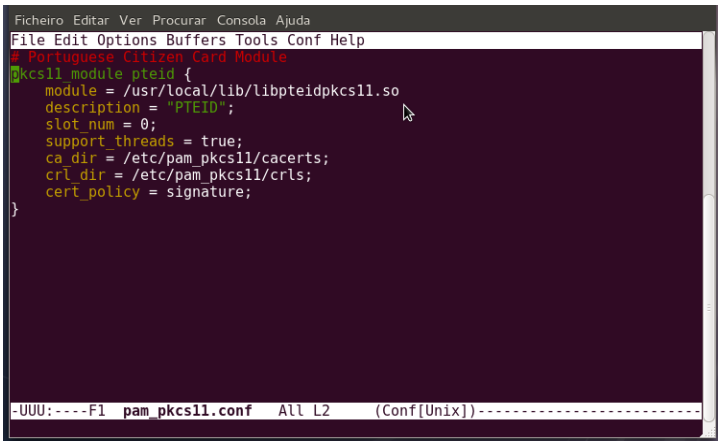
```
cd /etc/pam_pkcs11/cacerts
sudo cp /usr/share/ca-
certificates/mozilla/GTE_CyberTrust_Global_Root.crt .
sudo cp /usr/local/share/certs/ECRaizEstado_novo_assinado_GTE.der .
sudo cp /usr/local/share/certs/CartaodeCidadao001.der .
sudo pkcs11_make_hash_link
cd /etc/pam_pkcs11/crls
sudo wget
https://pki.cartaodecidadao.pt/publico/lrc/cc_ec_cidadao_crl001_crl.cr
l
```

Criar o ficheiro pam_pkcs11.conf:

```
sudo cp /usr/share/doc/libpam-
pkcs11/examples/pam_pkcs11.conf.example.gz /etc/pam_pkcs11/
cd /etc/pam_pkcs11/
sudo gunzip pam_pkcs11.conf.example.gz
sudo mv pam_pkcs11.conf.example pam_pkcs11.conf
```

Editar o ficheiro /etc/pam_pkcs11/pam_pkcs11.conf e adicionar o bloco

```
# Portuguese Citizen Card Module
  pkcs11_module pteid {
    module = /usr/local/lib/libpteidpkcs11.so
    description = "PTEID";
    slot_num = 0;
    support_threads = true;
    ca_dir = /etc/pam_pkcs11/cacerts;
    crl_dir = /etc/pam_pkcs11/crls;
    cert_policy = signature;
  }
```



e substituir a linha *use_pkcs11_module = opensc*; por *use_pkcs11_module = pteid;*

Insira o cartão no leitor e corra o comando *pkcs11_inspect* para verificar se os procedimentos anteriores correram com satisfação.

2 - Configurar o user mapping para associar o login ao cartão

Editar o ficheiro "/etc/pam_pkcs11/pam_pkcs11.conf", para usar o subject mapper, alterando a linha correspondente, de forma a ficar:

```
#use_mappers = digest, cn, pwent, uid, mail, subject, null;
use_mappers = subject;
```

No terminal execute o seguinte comando:

```
sudo cp /usr/share/doc/libpam-
pkcs11/examples/subject_mapping.example
/etc/pam_pkcs11/subject_mapping
```

Agora devemos saber qual o caminho para o certificado. Para isso fazemos o comando:

```
pkcs11_inspect

/C=PT/O=Cart\xC3\xA3o de Cidad\xC3\xA3o/OU=Autentica\xC3\xA7\xC3\xA3o
do Cidad\xC3\xA3o/OU=Cidad\xC3\xA3o Portugu\xC3\xAAs/SN=SOUSA
FERREIRA/GN=JOAQUIM PEDRO/serialNumber=BIXXXXXXXXX/CN=JOAQUIM PEDRO
SOUSA FERREIRA
```

ATENÇÃO - Vamos encontrar 4 ou 5 certificados, o que nos interessa é o de Autenticação (não os de assinatura), e aquele que inclui o nosso número de BI na descrição. Deve ser o primeiro, mas é melhor confirmar.

E supondo que queremos usar o cartão com o login "joaquim", editamos o ficheiro "/etc/pam_pkcs11/subject_mapping" e adicionamos a seguinte linha:

```
/C=PT/O=Cart\xC3\xA3o de Cidad\xC3\xA3o/OU=Autentica\xC3\xA7\xC3\xA3o
do Cidad\xC3\xA3o/OU=Cidad\xC3\xA3o Portugu\xC3\xAAs/SN=SOUSA
FERREIRA/GN=JOAQUIM PEDRO/serialNumber=BIXXXXXXXX3/CN= JOAQUIM PEDRO
SOUSA FERREIRA -> joaquim
```

4.2.1 Configurar o pam de forma a utilizar o módulo pkcs11

É necessário criar o ficheiro "/usr/share/pam-configs/pkcs11", com o seguinte conteúdo:

```
Name: Pam_pkcs11
Default: yes
Priority: 800
Auth-Type: Primary
Auth: sufficient pam_pkcs11.so
config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

De seguida executar:

```
sudo pam-auth-update
```

Garantimos que o módulo "Pam_pkcs11" está marcado na lista que surge e carregamos em "OK".

Vários ficheiros devem ser alterados, mas podemos confirmar se funcionou se no ficheiro "/etc/pam.d/common-auth", estiver algum conteudo semelhante:

```
...
# here are the per-package modules (the "Primary" block)
auth    sufficient pam_pkcs11.so
config_file=/etc/pam_pkcs11/pam_pkcs11.conf
auth    [success=2 default=ignore]      pam_unix.so nullok_secure
try_first_pass
...
```

Embora o mais importante é existir a linha:

```
auth    sufficient pam_pkcs11.so
config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

A partir deste momento todos os serviços que utilizem autenticação PAM vão, se detetarem o leitor ligado, pedir o PIN do certificado. Se não detectarem o leitor ligado pedem a senha normal.

Se usar o gestor de login gráfico *gdm* deverá ser possível realizar a autenticação, com recurso aos passos anteriores.

5 Notas do Utilizador